**Amendment**
**Published: February 27, 2015**
**Broad Agency Announcement Solicitation HSHQDC-14-R-B0016**
**Project: Cyber Physical System Security (CPSSEC)**

This amendment is identified in Federal Business Opportunities (FBO) as "Amendment 00011;" however, it is the first and only amendment to HSHQDC-14-R-B0016. The numbering for this amendment (Amendment 00011) is portrayed this way in FBO (rather than as the Amendment 00001 to HSHQDC-14-R-B0016) because this solicitation is posted in FBO as "Solicitation 2, CSD BAA CPSSEC" on the same FBO page as the overarching 5-yr CSD BAA, HSHQDC-14-R-B0005. Therefore, FBO identifies this as the next amendment in the sequence of all amendments issued to HSHQDC-14-R-B0005 or any solicitations/calls posted on the same page under the overarching CSD 5-yr BAA.

Changes to this solicitation are identified in red with change marks in the left hand margin.

## 1. Introduction

1.1 The overall goal of the Cyber Physical System Security (CPSSEC) project is to add necessary security enhancements to the design and implementation of cyber physical systems [1]. Cyber physical systems are smart networked systems that combine both cyber and physical technologies. Cyber physical systems play an integral role in the nation's critical infrastructure. Our transportation systems, emergency response systems, energy systems, and medical devices are rapidly adding cyber components to these existing physical systems.

1.2 Cyber physical systems represent a core opportunity area and source of competitive advantage for the innovation economy in the 21st century, but also represent an area where the consequences of cyber attacks could have severe impact on human lives and the environment. Executive Order 13636 [2] and Presidential Policy Directive 21 [3] state that proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure and include interdependent functions and systems in both the physical space and cyberspace.

1.3 This is a critical time in the design and deployment of cyber physical systems. Advances in networking, computing, sensing, and control systems have enabled a broad range of new devices. These systems are being designed and deployed now, but unfortunately security is often left as an additional feature that will be bolted on later. Industry is driven by functional requirements and fast moving markets. Cyber physical system designs are evolving rapidly and in most cases design standards are only now beginning to emerge. Many of the devices being deployed today have lifespans measured in decades. The design choices being made today will directly impact next several decades in transportation, emergency response, energy, medical devices, and so forth. This project aims to change the approach to cyber physical system design and ensure that we ***build security into the design*** of these critical systems.

## 2. Project Description/Scope

2.1 The premise of this project is that one needs to build security into the design of cyber physical system at an early stage. Emerging cyber physical system designs often have not been subjected to comprehensive threat analyses, have both known and unknown vulnerabilities, and lack security as an integral part of design. As these systems become widely deployed, the security issues will correspondingly increase and the systems will need to evolve to meet these threats. Security is not a feature that will emerge on its own. Past results have shown that adding security after systems are designed and deployed, i.e., "bolting security on", is challenging at best and at worst can have catastrophic consequences. Building security into the design entails identifying security considerations at the onset, enabling productive research and industry collaboration to balance security concerns and economic drivers, and ultimately adding security features as an integral part of cyber physical systems.

2.2 By definition, cyber physical systems combine both cyber and physical components. Any security design should make use of both the cyber and physical properties of the system. The physical world introduces constraints that could play a critical role in detecting invalid behaviors, discarding invalid data, and responding to threats. As a very simplistic example, a cyber physical system may include sensors that report physical properties, such as velocity, and there are physical constraints on velocity readings. A strong design might ensure that an attacker attempting to provide false readings from one sensor would also need to manipulate other sensor readings in order to dramatically change the sensor output. Overall, a strong security design should make use of both cyber and physical properties.

2.3 The CPSSEC project encourages applied research that bridges the gap between fundamental science and the growing set of cyber physical systems being produced. DHS recognizes the importance of cross cutting fundamental work that spans many different cyber physical system drivers and has partnered with the National Science Foundation on fundamental research in this area [9]. DHS also recognizes the importance of engaging industry to identify key requirements and challenges and is working to engage industry partners. This BAA call aims to help bridge the gap between fundamental science and the challenges facing industry.

2.4 To focus the research for this BAA call, DHS is seeking research to support security solutions related to the key drivers for cyber physical systems identified in the 2014 NITRD Cyber Physical Systems Vision Statement [1]. Therefore, offerors must clearly identify one (and only one) key driver as the basis for any submission to this BAA call. These drivers include transportation, manufacturing and industry, healthcare, energy, agriculture, defense, building controls, and emergency response. Offerors are encouraged to review the CPS Vision Statement [1] for additional information on the key drivers. Each driver brings its own set of requirements, economic realities, and security issues. Offerors should be cognizant of the resource constraints, economic realities, and most importantly, the security issues for the selected driver. DHS has interest in solutions that address any of these key driver areas; however, priority will be given to the transportation, emergency response, energy, and healthcare drivers. Further specialization within a key driver area is encouraged. For example, a solution could identify transportation as its key driver and further narrow its focus to specific challenges of automobiles, since the resource, economic, and security issues for automobiles may be substantially different from

those of aviation. This is intended only as an illustrative example. Technical approaches should narrow scope sufficiently so that resource constraints, economic realities, and security issues can be clearly identified and addressed.

2.5 This CPSSEC project BAA call is comprised of three complementary Technical Topic Areas (TTAs):

2.5.1 TTA #1, Security Models and Interactions
2.5.2 TTA #2, Secure System Design and Implementation
2.5.3 TTA #3, Experiments and Pilots

2.6 Each TTA is discussed in detail below and illustrative issues are identified for each; and as with all cyber physical systems work, technical approaches should address both the cyber aspects of the system and the physical aspects of the system.

# 3. Technical Topic Areas (TTAs)

## 3.1 TTA #1: Security Models and Interactions

3.1.1 Building security into cyber physical system designs requires an understanding of how cyber and physical system components are expected to interact. It is often not clear what interactions are expected, what interactions might occur, and there is often no reliable threat model. Even if interactions and threats are understood, methodologies for testing and validation are lacking. For example, vehicle sensors may detect obstacles and trigger braking actions or deployment of airbags. These cyber and physical interactions provide many of the key advances that drive cyber physical system deployment. At the same time, other unexpected interactions may occur and could be exploited by an adversary. Following the example, the vehicle's telematics system might interact with other devices and allow an adversary to incorrectly trigger braking. As the system designs emerge, it is essential to understand the potential interactions and identify corresponding threats. In addition, models are needed for testing and validation of cyber physical systems in order to verify that designs, especially security system designs, are performing as anticipated.

3.1.2 The following issues are considered particularly relevant for this TTA. These are only intended to be illustrative. Responses to this TTA may focus on one issue, address multiple issues, or address other issues relating to modeling interactions and threats.

3.1.2.1 Illustrative issue: Security Models and Taxonomies. Producing security models and taxonomies that allow one to understand the security of a cyber physical system is of interest to DHS. Models and taxonomies must address both the cyber and physical aspects of systems and understanding the interactions between the cyber and physical components is a key challenge. Any models produced should not simply list potential vulnerabilities; the goal must not be to simply document new ways to disrupt critical systems. Instead, the security models must provide actionable directions for addressing vulnerabilities and improving system security. Any directions must take into account the economic realities and the desired use cases. The models should allow one to understand and analyze trade-offs between potential threats,

economic costs, and desired use cases.

3.1.2.2 Illustrative issue: Combining Security with Safety. Adding security to systems that have primarily been designed for safety is also of interest to DHS. Many cyber physical systems were developed for environments with a long history of safety engineering. While safety and security share some common elements, there are also sharp differences between safety and security. As systems evolve from purely physical systems to cyber physical systems, the notion of safety for these systems changes and security must be included.

3.1.2.3 Illustrative issue: Metrics and Ratings. Metrics are often lacking and it is difficult to assess the current security state of a cyber physical system and even more challenging to demonstrate is the extent to which particular design choices impact security. No cyber physical system will ever be completely secure against all potential threats. Instead, different design choices may provide different levels of security. Techniques are needed to allow comparisons between different approaches and, if possible, provide quantitative metrics that can be used to assess or rate the security of designs and compare alternate approaches.

3.1.2.4 Illustrative issue: Building Codes for Cyber Physical Systems. Recent work has proposed the concept of "building codes" for software systems [4] and this concept extends to cyber physical systems. The physical world has an established history of quantifiable and checkable requirements. A building inspector does not need to be an expert architect, electrician, or plumber. Instead an inspector with general knowledge can verify that specific and quantifiable conditions are being met. These might include spacing between electrical outlets, level of insulation around piping, use of particular materials in structural components. These checks do not ensure a particular building is perfectly safe, but it is widely accepted that building codes have dramatically improved overall safety. As discussed above, safety and security are not equivalent and cyber physical systems are not equivalent to buildings. Of interest to DHS is whether the equivalent of building codes might be developed for cyber physical systems and how the building codes could be expressed and quantified.

3.1.2.5 Illustrative issue: Model-based Testing and Validation. Model-based techniques are needed to support security testing and validation for cyber physical systems. Within cyber physical systems, the interactions between physical and cyber components adds to the complexity of the systems, making it infeasible to exhaustively test all possible system states. Thus, DHS is interested in model-based techniques for testing and validating cyber physical systems, with a particular emphasis on models to assess the complex interactions within cyber physical systems as well their external interfaces.

3.1.3 In general for this TTA, technical approaches must identify how the models developed will be tested and evaluated. The testing and evaluation should be specific to the key driver identified and could include analysis, simulation, or extrapolation from experiments. Also, offerors should plan to deliver the first iteration of their security model within 6 months, and subsequently deliver further model updates every 6 months until the end of the award period of performance.

3.1.4 Data used to demonstrate capabilities and information sharing across awards resulting from this TTA is encouraged. Multiple performers using comparable data is beneficial to each individual performer since it can permit independent replication of results.

3.1.5 Further, in the context of this TTA, the commercialization and transition planning should be specific to the key driver and must describe cognizance of the operational policies and procedures commonly used by the key driver. A report discussing recommendations for real-world design and implementation changes based on models, that would be developed, is required no later than 6 months prior to the project end date.

3.1.6 Finally, all responses to this TTA must be specific to a key driver as discussed in Section 2 above, and provide a technical approach that would yield actionable information that can be adopted by industry.

3.1.7 Section 4.1 below identifies key deliverables for this TTA.

## 3.2 TTA #2: Secure System Design and Implementation

3.2.1 Current designs and implementations of cyber physical systems face challenges on how to include authentication and authorization, intrusion detection, intrusion tolerance and mitigation, and techniques for secure updates to cyber physical systems. The intent of this TTA is to addresses the question of building security into cyber physical system designs and implementation. For example, unfortunately it is not uncommon for cyber physical system designs to place all components on a shared network where it is simply assumed components will behave correctly; no authentication is provided, no monitoring takes place, and there is at best limited logging, It is not surprising that these systems have security vulnerabilities. Cyber physical system designs can benefit from traditional security concepts, such as authorization and authentication, anomaly based intrusion detection, signature based intrusion detection, monitoring and logging, and techniques for securely applying patches and updates.

3.2.2 Although one can apply traditional security concepts, designing cyber physical systems is not equivalent to traditional information technology security. By definition, cyber physical systems combine both cyber and physical components. A secure design for cyber physical system should take into account interactions between the cyber and physical system components and make use of both cyber and physical properties.

3.2.3 The following issues are considered particularly relevant for this TTA. These are only intended to be illustrative.

3.2.3.1 Illustrative issue: Authentication and Authorization. A key component of many secure designs is the ability to authenticate components, messages, and users, where appropriate. Similarly, authorization often plays a key role in secure system design. A design goal should be to implement techniques that provide appropriate levels of authentication and authorization based on cyber physical system architectures. In many cases, a necessary first step is to review cyber physical system architectures and computing capabilities to determine what permission levels might be needed and what might be feasible.

3.2.3.2 Illustrative issue: Monitoring and Logging. As cyber physical systems become widely deployed, it is essential that appropriate monitoring and logging be included in system design and implementations. In order to address security concerns, one must have access to some form of system data. If a compromise is suspected, one should be able to determine whether a compromise actually occurred and understanding the scope of the compromise if it did occur. This requires maintaining some form of system state. DHS is interested in determining what data should be monitored and logged, how it would be stored and accessed, and how it would be used in the event of either malfunction or compromise.

3.2.3.3 Illustrative issue: Intrusion Detection, Mitigation, and Tolerance. Extending the monitoring and logging issue above, ideally one would be able to detect when a compromise is occurring and take action to mitigate the threat. The system design may combine the ability to detect and mitigate threats with an expectation of intrusion tolerance. Subject to specific constraints of the key drivers, DHS is interested in approaches to guide design choices of when to mitigate and when to tolerate threats.

3.2.3.4 Illustrative issue: Secure Updates. Integrating information security into the complete cyber physical system lifecycle is a key challenge. Provisions for making security updates to cyber physical systems throughout their life, including reasonable assumptions on human factors, providing interfaces to security features, and anticipating human error are all elements system security lifecycle. A cyber physical device such as a vehicle, Supervisory Control and Data Acquisition (SCADA) system, or medical device may have a lifetime measured in decades and updates to the system are inevitable. Therefore, DHS is interested in technical approaches that address how to securely update the security posture of a cyber physical system.

3.2.4 In general for this TTA, technical approaches include a plan for testing and evaluation of prototype designs and operation meet the goals of the TTA, potentially via addressing an illustrative issue. The testing and evaluation should be specific to the key driver identified and could include analysis, simulation, or extrapolation from experiments. Also, offeror's should plan to provide initial design requirements within 6 months, a prototype implementation within 12 months, and then subsequent updates to the design and prototype every 6 months.

3.2.5 Data used to demonstrate capabilities and information sharing across awards resulting from this TTA is encouraged. Multiple performers using comparable data is beneficial to each individual performer since it can permit independent replication of results.

3.2.6 Further, in the context of this TTA, the commercialization and transition planning should be specific to the key driver and must describe cognizance of the operational policies and procedures commonly used by the key driver.

3.2.7 Referring to the issues above, responses to this TTA may focus on one issue, address multiple issues, or address other issues not mentioned relating to secure system design and implementation. However, all responses to this TTA must be specific to a key driver as discussed in Section 2 above, and provide a technical approach that would yield actionable

information that can be adopted by industry.

3.2.8 Section 4.2 below identifies key deliverables for this TTA.

## 3.3 TTA #3: Experiments and Pilot Projects

3.3.1 The CPSSEC project aims to bridge the gap between advances in fundamental science and the cyber physical systems being deployed today. Cyber physical systems (CPS) are being deployed and used today and must not be viewed only as future systems. For example, cyber physical systems are not limited to the autonomous vehicles being explored by research labs. The vehicles available today include a growing set of cyber physical components, including lane change sensors, adaptive cruise control, forward collision warning, integrated telematics systems, and so forth. Similarly, energy, emergency response, healthcare, and the other key driver areas include cyber physical systems that are being deployed and used today.

3.3.2 DHS and other operational components need experimental deployment opportunities to investigate operational capabilities of new cyber physical system security technologies. Thus, the objective of this TTA is to provide an opportunity to analyze early (and potentially mature) designs through experiments and pilots; and also create a cyber physical system specific framework and methodology to evaluate the cyber security properties of a cyber physical system prior to operational deployment. This TTA will facilitate experiments or pilot deployments of CPS, in either government or commercial settings, for the purpose of measuring and documenting their respective information system security postures. Therefore, to support the objective of this TTA, offerors are encouraged to propose evaluations of cyber physical systems relevant to the Homeland Security Enterprise and the aforementioned key drivers, especially first responders, subject to the following key challenges.

3.3.3 First, the technical readiness level (TRL) of the system under test should be clearly defined and the approach to evaluation should align with the TRL. Also, the evaluation must clearly explain what level of expertise is expected from the experiment or pilot project participants.

3.3.4 Second, safety concerns must be clearly identified and appropriate risk mitigation must be explained. Experiments and pilots in realistic settings can be much more valuable than strictly isolated experiments. However, typical cyber physical systems such as vehicles, energy systems, medical devices, and emergency response systems, are all systems that directly impact people's lives. The first priority of any pilot or experiment must be to ensure the safety of the participants as well as anyone else who might come in contact with the pilot or experiment. Therefore, offeror's need to be compliant with DHS Protection of Human Subjects [10] directives for any proposed experiment or pilot.

3.3.5 Third, any experiment or pilot should clearly explain how cyber attacks would be introduced and the lessons learned from a cyber security perspective should be clearly identified. Experiments and pilots should have clear questions that will be evaluated and clear metrics to assess the level of success. Whenever possible, experiments should be repeatable and independently verifiable so that competing designs could execute similar tests and provide

comparable results.

3.3.6 For planning purposes, it is expected that within 6 months of award, a report on experiment/pilot metrics along with a security analysis plan. Initial results should be available in a test report delivered not later than 12 months from award. Depending on the system under test, offerors may want to consider optional evaluations beyond 12 months of award. In this case offerors should plan to provide subsequent updates of deliverables every 6 months.

3.3.7 Data used to demonstrate capabilities and information sharing across awards resulting from this TTA is encouraged. Multiple performers using comparable data is beneficial to each individual performer since it can permit independent replication of results.

3.3.8 Section 4.3 below identifies key deliverables for this TTA.

# 4. Project Structure

The CPSSEC project will be organized based on key drivers from the following list:

- Transportation
- Emergency Response
- Energy
- Healthcare
- Building Controls
- Manufacturing and Industry
- Agriculture
- Defense

## 4.1 TTA #1 Key Deliverables

The key deliverables required for TTA #1 are:

| **DELIVERABLES** | **DUE DATE** |
|---|---|
| Quarterly Technical Status Reports | 3 months after award |
| Initial Model Specific to a Key Driver | 6 months from project start |
| Subsequent Model Updates | every 6 months |
| Recommendations for Design Changes | 6 months prior to project completion |
| Final Report | project completion |

## 4.1 TTA #2 Key Deliverables

The key deliverables required for TTA #2 are:

| **DELIVERABLES** | **DUE DATE** |
|---|---|
| Quarterly Technical Status Reports | 3 months after award |
| Test and Evaluation Plan | 6 months from award |
| Design Requirements Specific to Key Driver | 6 months from award |
| Subsequent Design Updates | every 6 months |
| Prototype Implementation | no later than 12 months from |

| | |
|---|---|
| | project start |
| Subsequent Prototype Updates | every 6 months |
| Final Report | project completion |

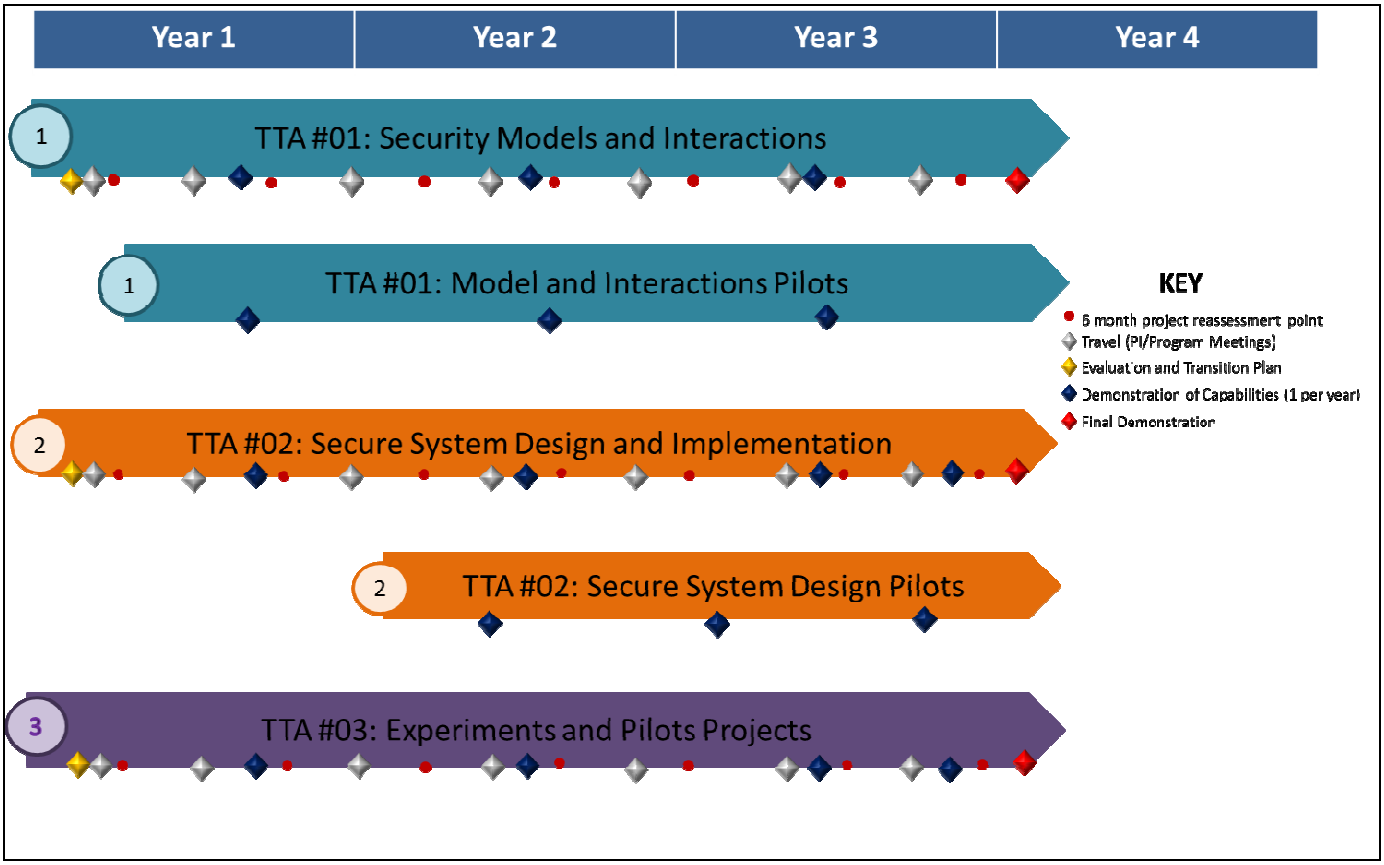
### 4.2 TTA #3 Key Deliverables

The key deliverables required for TTA #3 are:

| DELIVERABLES | DUE DATE |
|---|---|
| Initial Assessment of Technical Readiness Level | 1 month after award |
| Quarterly Technical Status Reports | 3 months after award |
| Pilot and Experiment Test Plan | 3 months from award |
| Report on Metrics and Plan for Security Analysis | 6 months from award |
| Pilot Project or Experiment Initial Results | no later than 12 months from project start |
| Subsequent Prototype Updates | every 6 months |
| Final Report | project completion |

## 5. Project Schedule/Milestones

A notional project schedule is shown below including anticipated meetings and demonstrations.



# 6. Special Instructions/Notifications

## 6.1 Response Dates

| Event | Time Due | Date or Date Due |
|---|---|---|
| Industry Day | N/A | June 26, 2014 |
| White Papers Due | 4:30 PM EDT | July 22, 2014 |
| Notification of White Paper Evaluation Results | N/A | On or About August 29, 2014 |
| Proposals Due | 4:30 PM EDT | ~~September 30, 2014~~ March 30, 2015 |

## 6.2 General Instructions and Information

6.2.1 This BAA solicitation (HSHQDC-14-R-B0016, as amended) includes a requirement to submit white papers, prior to the submission of proposals, subject to the date identified in the "Response Dates" table above.

6.2.2 Procedures for submission of white papers and proposals in the DHS S&T Portal are provided in paragraph 10 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003. Note that offerors must complete the company/organization portal registration PRIOR to submitting a white paper for the first time. Ensure adequate time to complete the company/ organization registration as delays in this process will not be authorization for late submissions of white papers. Company/organization registration information is located in paragraph 10.1 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003. In addition, each white paper and subsequent proposal requires registration in the portal. Information regarding white paper and proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003.

6.2.3 Offerors may provide multiple white paper and proposal submissions; however, each submission must only address one TTA and must be distinct and self-contained without any dependencies on other work of any kind. Each submission must clearly state which TTA is being addressed.

6.2.4 All software developed and delivered is required to be subject to security auditing; therefore, the offeror's technical approach must identify how security auditing will occur. Also, DHS expects offerors to follow best practices on software design and encourages the use of the DHS Software Assurance Marketplace [6].

6.2.5 DHS has a strong preference for open source licensing of software for all software developed and delivered and the licenses for all proposed software deliverables will have to be identified in submitted white papers and proposals (note: the DHS HOST [7] project provides directions and opportunities for promoting open source software). However, as an alternative to open source release, offerors may also offer a strong technical transition plan for deployment of the technologies developed.

6.2.6 As stated in DHS S&T CSD BAA HSHQDC-14-R-B0005, Amendment 00003, DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to this BAA solicitation.

6.2.7 The Evaluation Criteria in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003 [3] Section 11 "EVALUATION OF WHITE PAPERS AND PROPOSALS" applies.

## 6.3 Foreign Participation

Offerors are reminded that foreign participation may occur as defined in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, Section 1.3. Therefore, for offerors should provide unit costs for any deliverable not anticipated for delivery in a softcopy format.

## 6.4 Export Control Requirements

Offerors are reminded of the export control markings required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, Section 8.6.8 (for white papers) and Section 9.6.4 (for proposals).

## 6.5 Type Classification Ceilings

DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, describes the Type Classifications for proposals. Specific to this call, the ceiling values for each type are as follows:

6.5.1 Type I – Type I awards are limited to a total contract value not to exceed $3,000,000.00, not including operational evaluation, pilot, and/or transition options.

6.5.2 Type II – Type II awards are limited to a total contract value not to exceed $2,000,000.00, not including operational evaluation, pilot, and/or transition options.

6.5.3 Type III – Type III awards are limited to a total contract value not to exceed $750,000.00, not including operational evaluation, pilot, and/or transition options.

## 6.6 Travel

6.6.1 For purposes of estimating costs for white papers and proposals, offerors should anticipate travel to 3 project meetings per year.

6.6.2 DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded efforts are expected to present. Projects will be required to provide a briefing, typically 20 minutes, and are strongly encouraged to provide demonstrations when appropriate. The PI meeting is typically 2.5 days and attendance at the full event is encouraged.

6.6.3 In addition to the annual DHS PI Meeting, the CPSSEC Project will hold two meetings each year. Meetings will be arranged by TTA and the meeting for each TTA is expected to last

one day. When possible, TTA meetings will be held on adjacent days so funded efforts in one TTA can optionally attend other TTA meetings.

## 6.7 White Paper Requirements

This BAA solicitation (HSHQDC-14-R-B0016, as amended) requires the submission of a white paper, compliant with the aforementioned response dates, to be considered for participation in the submission of proposals. Offerors MUST submit a white paper in accordance with the Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-14-R-B0005, Amendment 00003. Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count).

## 6.8 Proposal Requirements

To be considered for award, offerors **MUST** submit a proposal, compliant with the aforementioned response dates, in accordance with the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003. Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003 may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count). The DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003 [3] Section 9 discusses proposal preparation and describes the required proposal content; however, in addition to the guidance in Section 9, the following special instructions are added:

6.8.1 Maximum Page Count.

6.8.1.1 Volume 1 – Technical Proposals.

6.8.1.1.1 For any proposal submitted in response to this solicitation/call, Volume 1, the technical proposal, ***SHALL NOT*** exceed 30 pages. This maximum page count of 30 pages includes ***all*** information required to be included in Volume 1 of any submitted technical proposal. Information required to be included in Volume 1, Technical Proposal, is outlined in Sections 9.6.1(a) through 9.6.1(v) of BAA HSHQDC-14-R-B0005, Amendment 00003.

6.8.1.1.2 Notwithstanding any language used in BAA HSHQDC-14-R-B0005, Amendment 00003, Sections 9.6.1(a) through 9.6.1(v), such as "appendix", "resumes", etc., ***all*** required information in these sections counts towards the maximum page count of 30 pages. This includes the required "Cover Page", "Table of Contents", "Official Transmittal Letter", "Quad Chart", "Resumes", "Assertion of Data Rights", and so on, identified in Sections 9.6.1(a) through 9.6.1(v) of BAA HSHQDC-14-R-B0005, Amendment 00003.

6.8.1.1.3 Any Volume 1, Technical Proposal, received in response to this solicitation/call exceeding the maximum page count of 30 pages ***WILL NOT BE EVALUATED AND THEREFORE, WILL NOT BE ELIGIBLE FOR AWARD.***

6.8.1.2 Volume 2 - Cost Proposals. ***THERE IS NO PAGE COUNT LIMITATION FOR VOLUME 2, PRICE/COST PROPOSAL SUBMISSIONS.*** Information required to be included in any submitted Volume 2, Cost Proposal, is outlined in Sections 9.6.2(a) through 9.6.2(c) of BAA HSHQDC-14-R-B0005, Amendment 00003.

6.8.2 Subcontractor Cost Submission: Referencing, DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, Section 9.6.2.b.(6), if the subcontractor costs cannot be included with a prime's detailed cost breakdown, then the prime contractor must stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor's costs are provided separately as an attachment to an e-mail sent to BAA-14-R-B0005@hq.dhs.gov. The subject line of the email shall say "Separate Subcontractor Cost Submission – [insert the white paper or proposal number assigned from the DHS S&T BAA Portal]". The body of the email shall contain the following:

1) The prime entities name which should be the same entity that is registered in the BAA portal;
2) A POC (name and phone number) from the prime entity; and
3) For each subcontractor proposal attached, include:
   - The name of the subcontractor for the subcontractor proposal attached; and
   - A POC (name and phone number) from the subcontractor whose proposal is attached.

The separate subcontractor cost proposal must be as detailed as the offerors's cost proposal and must be received at the location designated in the individual call no later than the closing date and time specified by the call. Note that email transmission time may vary depending on the file size of the attachment(s) included in the email. Therefore, ensure there is adequate time for receipt of the email and any accompanying attachments of the subcontractor(s) cost proposal(s) by the required closing date and time. Acceptance of the email submission is dependent upon the actual date and time the e-mail and any accompanying attachment(s) is RECEIVED by the in-box for BAA-14-R-B0005@hq.dhs.gov. **NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE.**

## 6.9 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (HSHQDC-14-R-B0016, as amended) must be emailed to BAA-14-R-B0005@hq.dhs.gov no later than 4:30 PM EDT on March 30, 2015. Emails submitting questions are to include "Questions for CPSSEC BAA Solicitation" in the subject line. All questions and responses will be posted on the Federal Business Opportunities website http://www.fbo.gov. Questions will only be accepted and answered electronically.

## 6.10 Order of Precedence

Additional Information: In the event that any of the terms and conditions contained in this solicitation (HSHQDC-14-R-B0016, as amended) conflict with terms and conditions included in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, the terms and conditions in this BAA solicitation (HSHQDC-14-R-B0016, as amended) shall take precedence.

## Footnotes:


1. 2014 NITRD Cyber Physical Systems Vision Statement; http://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf
2. Executive Order 13636, Improving Critical Infrastructure Cyber Security; http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
3. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience; http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
4. Carl E. Landwehr," A building code for building code: putting what we know works to work", Annual Computer Security Applications Conference, ACSAC '13, New Orleans, LA, USA, December 9-13, 2013; http://dx.doi.org/10.1145/2523649.2530278
5. DHS Cyber Security Division Broad Agency Announcement HSHQDC-14-R-B0005; https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-14-R-B0005/listing.html
6. DHS Software Assurance Marketplace (SWAMP); https://continuousassurance.org/
7. DHS Homeland Open Security Technologies (HOST); https://www.dhs.gov/csd-host
8. DHS Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT); https://www.predict.org
9. Cyber-Physical Systems (CPS) Program Solicitation NSF 14-542; http://www.nsf.gov/pubs/2014/nsf14542/nsf14542.htm
10. Department of Homeland Security, DHS Directives System, MD Number: 026-04, Revision Number: 00, Issue Date: 05/25/2007; https://www.dhs.gov/xlibrary/assets/foia/mgmt-directive-026-04-protection-of-human-subjects.pdf